

PANORAMA DE LA MENACE INFORMATIQUE 2021

1.9.1

9 mars 2022



TLP:WHITE

Sommaire

Synthèse

Dans ce panorama de la menace informatique, l'ANSSI revient sur **les grandes tendances** ayant marqué le paysage cyber sur l'année **2020-2021** et en propose des **perspectives d'évolution à court terme**. Ces tendances s'inscrivent dans une hausse continue du niveau de menace. Ainsi, l'ANSSI a eu connaissance de 1082 intrusions avérées dans des systèmes d'information en 2021, pour 786 en 2020. Cela représente une hausse de 37 % des intrusions avérée dans l'année. Cette hausse s'explique par l'évolution et **l'amélioration constante des capacités des acteurs malveillants** dont les principales intentions restent le **gain financier, l'espionnage et la déstabilisation**. Ces acteurs ont su saisir une **multitude d'opportunités offertes par la généralisation d'usages numériques souvent mal maitrisés**. Une vigilance particulière est par conséquent nécessaire dans le cadre d'évènements majeurs en France tels que la présidence française de l'Union européenne, les élections présidentielles et législatives en 2022 et les Jeux Olympiques de Paris 2024 qui sont autant d'opportunités contextuelles à exploiter pour des attaquants.

L'évolution de l'écosystème cybercriminel est marquée par une professionnalisation et une spécialisation constantes, cause et conséquence de la maturité et des gains financiers acquis par ses acteurs. Les rançongiciels vendus en tant que service (*RaaS*) et les entreprises peu regardantes qui offrent à des acteurs malveillants des capacités d'hébergement (*Bullet Proof Hosters*) en sont une parfaite illustration. Les acteurs cybercriminels adoptent également des modes opératoires semblables à ceux d'acteurs soutenus par des gouvernements, en préparant minutieusement leurs opérations, en persistant sur les réseaux de leurs victimes pendant de longues périodes à la recherche de ressources d'intérêt et parfois en exploitant des vulnérabilités inconnues *0-Day*. Par ailleurs, cette mise à disposition d'outils et services malveillants prêts à l'emploi pourrait profiter à d'autres types d'attaquants, notamment motivés idéologiquement tels que les hacktivistes.

Les attaquants étatiques s'inspirent également des méthodes cybercriminelles en s'appropriant des codes et outils traditionnellement utilisés par les attaquants cybercriminels tels que des rançongiciels ou des techniques d'hameçonnage. Pour se dissimuler, ils exploitent des outils légitimes présents sur les réseaux des victimes, échappant ainsi à la détection (selon la technique du *living-off-the-land - LotL*). Cette **porosité entre différents profils d'attaquants** complique la caractérisation des activités malveillantes.

Le développement de capacités offensives par des entreprises privées telles que NSO Group rendent accessibles des capacités parfois de pointes à des acteurs n'ayant pas les moyens de les développer ou souhaitant maintenir une possibilité de déni plausible. Cette mise à disposition de capacités avancées parfois très sophistiquées participe à la hausse générale du niveau de menace en multipliant ses sources et en favorisant un usage décomplexé des cyberattaques.

Si les attaques à finalité lucrative ont occupé la scène médiatique, elles ne doivent pas occulter les campagnes d'espionnage, par essence moins visibles, et celles conduites dans un objectif de sabotage informatique.

L'**espionnage informatique** reste **la principale finalité poursuivie** par les attaquants étatiques et constitue l'essentiel de l'activité traitée dans le cadre des opérations de cyberdéfense conduites par l'ANSSI. Dans certains cas, l'espionnage informatique peut être **facilité par la mise en place ou le détournement de dispositifs juridiques**.

Le ciblage d'infrastructures critiques reste également une **préoccupation majeure**. Plusieurs acteurs cybercriminels ont ainsi ciblé sur le territoire français des hôpitaux à l'aide de rançongiciels paralysant l'activité de structures vitales. La multiplication des opérations de démantèlement, les arrestations de réseaux cybercriminels menées par le biais de coopérations internationales ainsi que les prises de position de plusieurs États, notamment les États-Unis, semblent avoir eu un effet sur le ciblage des infrastructures critiques. Les cybercriminels pourraient ainsi éviter de compromettre volontairement ce type de structure dans un avenir proche. Cependant leur ciblage par des acteurs réputés étatiques devrait se poursuivre en partie en cas de tensions géopolitiques fortes comme entre Israël et l'Iran où plusieurs infrastructures critiques ont fait l'objet d'attaques informatiques (approvisionnement en eau, en énergie). Des entités françaises implantées à l'étranger pourraient ainsi être des victimes collatérales de ce type d'opérations.

Enfin, **des attaques informatiques mises à profit d'opérations d'influence et de déstabilisation** sont à anticiper notamment à l'approche d'évènements majeurs en France. En effet, de plus en plus d'opérations informationnelles

s'appuient sur des compromissions informatiques permettant d'exfiltrer des documents et d'obtenir des accès initiaux, à l'image de la campagne « Ghostwriter ». Cette campagne a été attribuée à la Russie par de nombreux partenaires de l'ANSSI et a touché, entre autres, la Pologne et l'Allemagne en 2021.

Que ce soit dans le cadre d'opérations d'extorsion, d'espionnage, d'influence ou de déstabilisation, les attaquants bénéficient pleinement de la fragilité des infrastructures numériques.

L'année 2020-2021 a ainsi vu une **explosion du nombre de vulnérabilités *0-Day*** exploitées, majoritairement par des acteurs étatiques, mais également par quelques groupes cybercriminels notamment au cours de l'attaque du 2 juillet 2021 contre le fournisseur de solution d'administration à distance Kaseya. Ce dernier exemple rappelle également qu'une attention particulière doit être accordée aux **attaques ciblant la chaine d'approvisionnement** (*supply chain*), une méthode particulièrement prisée par les attaquants. Cette tendance présente des risques de propagation rapide depuis un éditeur de logiciels ou une entreprise de services numériques ciblés, avec un risque de compromission en cascade. Les attaquants ont également su tirer profit des nouveaux **usages numériques souvent mal maitrisés tels que le *Cloud*** à des fins lucratives et d'espionnage.

La multiplication des attaques informatiques a conduit à une explosion des fuites de données notamment personnelles. Qu'elles soient issues de divulgations effectuées par des opérateurs de rançongiciels, d'opérations de déstabilisation ou de revente d'informations par des cybercriminels, ces données alimentent un cercle vicieux. En effet, elles facilitent de nombreuses attaques informatiques en fournissant des portes d'entrée aux attaquants.

La propagation rapide à l'ensemble d'un système d'information peut être entravée par deux mesures de défense principales :

- la protection des administrateurs systèmes, en particulier pour les domaines Active Directory. Leurs comptes d'administration ne doivent idéalement jamais être utilisés pour un usage de navigation internet, de messagerie ou de bureautique ;
- la segmentation réseau stricte, limitant les possibilités de flux entre des zones dédiées à des usages différents (par exemple selon les métiers, les emprises géographiques ou la typologie des machines).

L'utilisation de gestionnaires de mot de passe, l'activation généralisée de l'authentification à multiples facteurs et une sensibilisation des utilisateurs aux mots de passe forts pourraient réduire significativement les possibilités des attaquants. Une révision des politiques de mise à jour au sein des organisations et le cloisonnement des réseaux permettraient également de ralentir voire éviter de nombreuses attaques informatiques.

L'ANSSI vous invite à consulter les guides « Recommandations relatives à l'authentification multifacteur et aux mots de passe » (https://www.ssi.gouv.fr/administration/guide/recommandations-relatives-a-lauthentification-multifacteur-et-aux-mots-de-passe/) et « Attaques par rançongiciels, tous concernés - Comment les anticiper et réagir en cas d'incident » (https://www.ssi.gouv.fr/administration/guide/attaques-par-rancongiciels-tous-concernes-comment-les-anticiper-et-reagir-en-cas-dincident/).

1. Des acteurs offensifs aux capacités en constante progression

1.1. Cybercriminalité : spécialisation et professionnalisation des acteurs

À l'image de la criminalité organisée traditionnelle, la cybercriminalité constitue un réseau économique associant des fournisseurs de services spécialisés dont les membres collaborent plus ou moins étroitement en fonction des opportunités et des objectifs du moment. Cette organisation est à la fois la cause et la conséquence de la maturité qu'a atteint l'écosystème cybercriminel, alimenté directement par ses gains financiers, estimés à plus d'un milliard d'euros par an.

Cet écosystème s'est spécialisé autour d'une galaxie de métiers et de rôles correspondant souvent aux différentes étapes d'une attaque informatique. Les acteurs cybercriminels se spécialisent ainsi en fournisseurs de services proposant des codes malveillants, des infrastructures d'anonymisation, des accès à des réseaux compromis (*Access Broker*), des réseaux de machines zombies *botnet*, des services d'envoi de pourriels ou encore de blanchiment d'argent. Très peu de groupes cybercriminels possèdent en interne l'ensemble de ces compétences. Ces groupes sont cependant susceptibles de fournir plusieurs types de services à l'image d'Evil Corp qui opère à la fois des rançongiciels depuis 2017 et distribue la porte dérobée Dridex [1] [2].

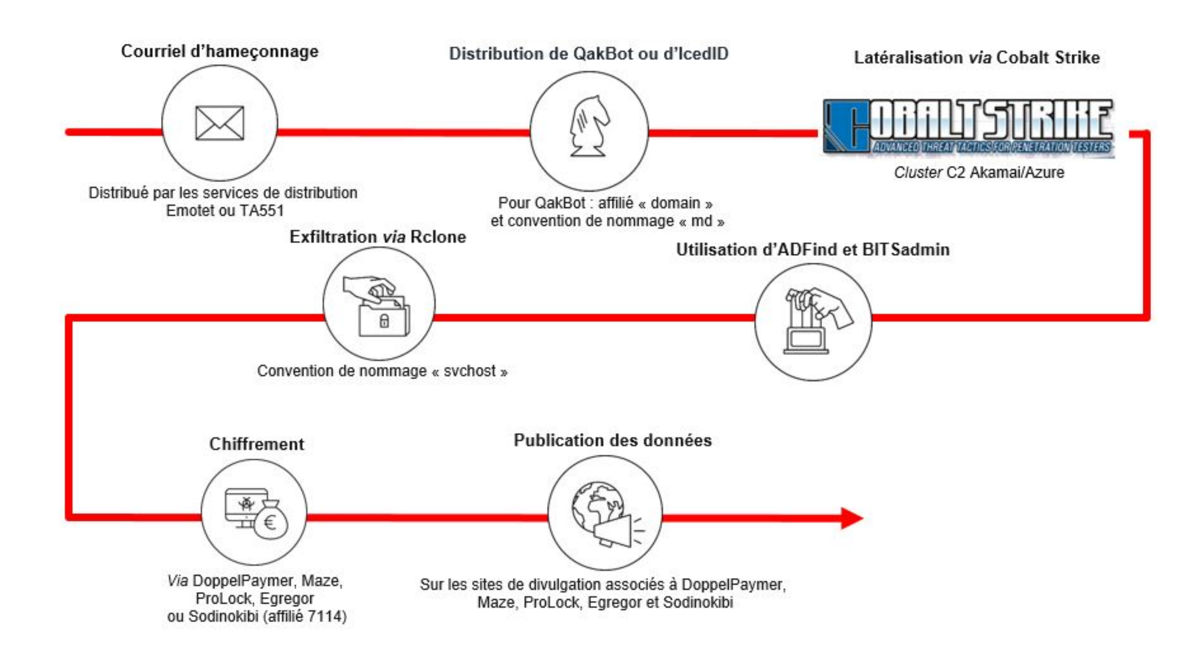


Fig. 1.1. – Chaîne d'infection récapitulative associée au groupe cybercriminel Lockean.

Cette spécialisation et ces offres de services entrainent une multiplication des chaînes d'infection potentielles et compliquent leur détection et leur suivi. Toutefois, certains services malveillants à l'image d'Emotet [3] ou encore Cobalt Strike deviennent des codes ou des nœuds d'infrastructures très répandus dont le suivi et le blocage permettent ainsi d'arrêter une attaque dès les premières étapes de la chaine d'infection.

Les *Bullet Proof Hosters* (« Hébergeurs pare-balles ») illustrent aussi parfaitement ce phénomène de spécialisation. Ces hébergeurs sont ainsi particulièrement conciliants vis-à-vis de leurs clients, en fournissant des services largement utilisés par des acteurs malveillants. Ces hébergeurs se caractérisent par :

- une politique de *Know Your Client* (KYC) inexistante ;

- un paiement en cryptomonnaies ;
- l'offre fréquente d'un service de changement de DNS très rapide ou DNS *Fast Flux* ;
- un contrôle inexistant voire la promotion explicite d'activités malveillantes ;
- un hébergement des infrastructures dans des juridictions hors d'atteinte des traités de coopération judiciaire.

Ces hébergeurs « pare-balles » sont utilisés par de nombreux groupes cybercriminels pour louer des ressources techniques. Plusieurs d'entre eux ont fait l'objet d'investigation en source ouverte comme Yalishanda [4], Dr. Samuil [5] , CCWeb ou encore BraZZZerS [6].

Commentaire : Un blocage préventif de leurs sous-réseaux voire des systèmes autonomes correspondant (Autonomous Systems - AS) peut améliorer grandement la sécurité d'une organisation. Cependant, des effets de bord sont possibles.

Les rançongiciels et notamment ceux vendus en tant que service (*Ransomware-a-a-Service* - RaaS) illustrent également ces phénomènes de spécialisation et professionnalisation de l'écosystème cybercriminel. Ils font intervenir un ensemble de groupes et de personnes, parfois spécifiquement recrutées en fonction de leurs compétences à l'instar de FIN7 [7]. Un revendeur d'accès ou *access broker* peut ainsi procéder à des scans de vulnérabilités pour identifier des cibles potentielles, en moyenne dans un délai de 48 h après la divulgation d'une vulnérabilité et d'une méthode d'exploitation. Ce revendeur peut également opérer un service d'hameçonnage ciblé ou non qui reste le vecteur de primo-infection le plus courant. Les accès ainsi obtenus sont partagés à d'autres attaquants, disposant par exemple d'expertise dans la latéralisation au sein de réseaux gérés par les annuaires *Active Directory*, composants critiques des systèmes d'informations. Une fois les ressources d'intérêt identifiées et exfiltrées, le chiffrement du parc informatique peut être lancé grâce au rançongiciel mis à disposition par les opérateurs du rançongiciel.

En 2021, l'ANSSI a suivi en moyenne une quarantaine de rançongiciels différents.

Ciblant l'ensemble des secteurs d'activité, cette menace reste majoritairement opportuniste et recherche des cibles peu sécurisées, disposant de ressources financières importantes et ne supportant pas de rupture d'activité. Il existe toutefois des subtilités dans le ciblage. Si certains groupes cherchent à maximiser leur profit en ciblant le plus de victimes possible, d'autres ne ciblent que de grandes sociétés particulièrement rentables dans le cadre d'opérations dites de *Big Game Hunting*. Ces variations se retrouvent également dans la rapidité de la chaine d'infection, de la phase de déploiement et de chiffrement. Certains groupes d'attaquants cybercriminels peuvent cependant rester plusieurs jours ou plusieurs semaines dans les réseaux de leurs victimes afin d'identifier les ressources clés, d'en étudier le contenu avant exfiltration et menace de publication pour exercer une pression supplémentaire lors de la phase d'extorsion et de négociation de la rançon.

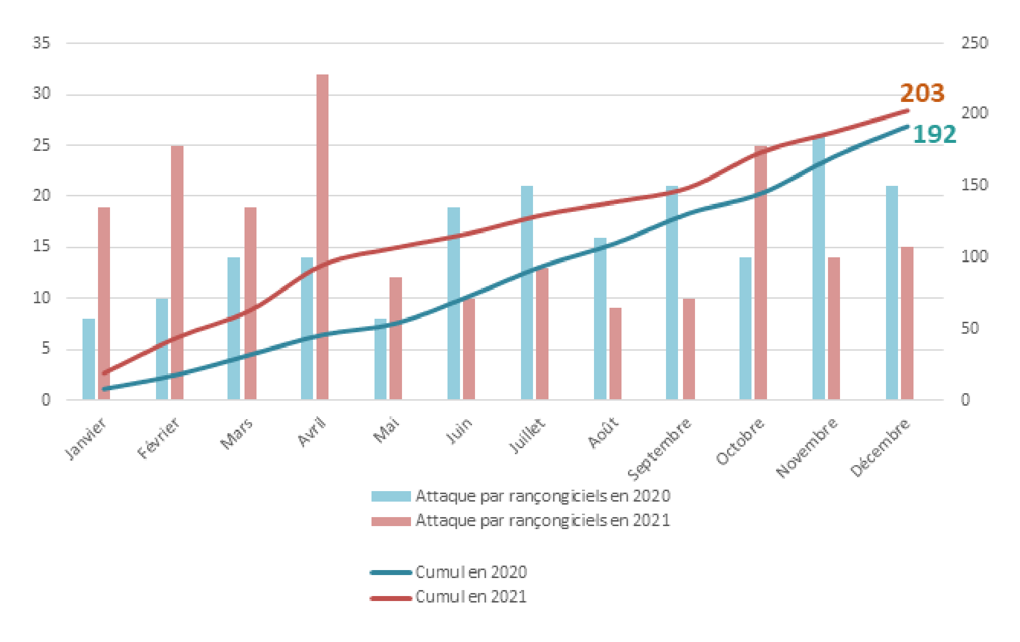


Fig. 1.2. – Statistiques concernant les attaques par rançongiciels traitées par l'ANSSI en 2020 et 2021.

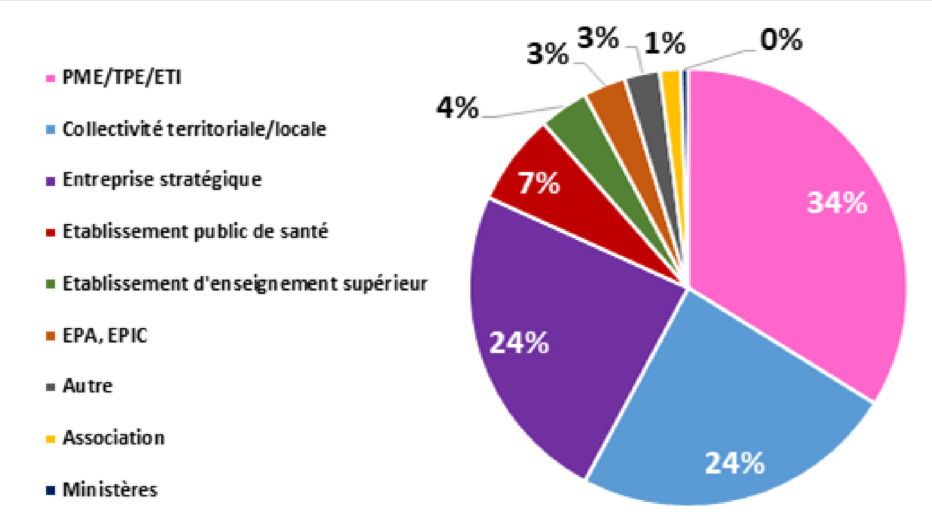


Fig. 1.3. – Répartition des entités victimes d'attaques par rançongiciel dans le cadre des incidents traités par l'ANSSI en 2020.

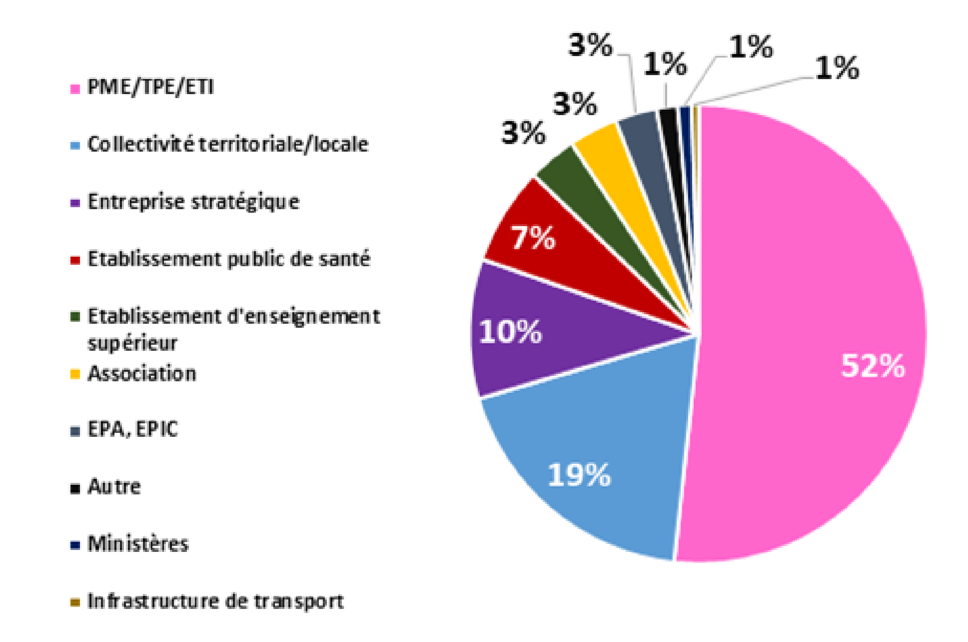


Fig. 1.4. – Répartition des entités victimes d'attaques par rançongiciel dans le cadre des incidents traités par l'ANSSI en 2021.

La multiplication des méthodes d'extorsion et des moyens de chantage mis en œuvre par les cybercriminels témoigne également de leur professionnalisation. Ces derniers n'hésitent pas à associer à la menace de divulgation de données exfiltrées, du chantage au DDoS [1], du harcèlement téléphonique ou encore des prises de contact avec des médias, des partenaires ou des clients de la victime, ce qui s'apparente à une certaine forme de « *Name & Shame* ».

Le ciblage de certains groupes pourrait évoluer pour éviter la compromission d'infrastructures critiques ou d'institutions publiques importantes. L'état d'urgence énergétique déclaré à la suite de la compromission de l'entreprise américaine Colonial Pipeline par le rançongiciel DarkSide [8] en mai 2021 et l'élévation du niveau d'alerte associé

1. Principe consistant à menacer une victime de réaliser des attaques répétées par déni de service à l'encontre de ses services en ligne si elle ne paye pas la rançon.

aux rançongiciels à un niveau équivalent à celui du terrorisme aux États-Unis [9] en juin 2021 ont marqué un tournant dans la prise en compte de cette menace à l'échelle internationale. Les moyens mis en œuvre par les forces de sécurité ont décuplé et les actions coup de poing se sont multipliées au cours de l'année 2021 : démantèlements de botnets, arrestations d'affiliés, récupérations de rançons, etc. **Ainsi, l'ANSSI estime que seuls les groupes d'attaquants en capacité de se mettre hors de portée des forces de sécurité, parfois grâce à la protection d'États, continueront à mener ce type d'attaques contre des organisations de dimension internationale. D'autres opérateurs de rançongiciels pourraient en réponse s'orienter vers du « simple » chantage à la divulgation d'informations exfiltrées.**

Toutefois, le réinvestissement des gains accumulés par les cybercriminels leur permettra très probablement d'acquérir de nouvelles capacités, compétences et outils adaptés à d'autres environnements techniques sur lesquels les capacités d'investigation peuvent être moins développées, comme Linux ou encore l'Internet des Objets (*Internet of Things* ou IoT).

1.2. Des acteurs étatiques de moins en moins identifiables

Depuis quelques années, l'ANSSI observe une convergence des méthodes et outils utilisés par plusieurs profils d'acteurs malveillants. Les acteurs étatiques utilisent désormais de manière plus courante des outils non-marquants, tels que Cobalt Strike, largement utilisés dans l'écosystème cybercriminel. Ce fut notamment le cas lors de la campagne d'espionnage contre des entités françaises en 2021 et mettant en œuvre le mode opératoire APT31 [10]. Ce phénomène n'est pas nécessairement organisé ou issu d'un rapprochement entre ces deux types d'acteurs bien que certains services de renseignements soient parfois accusés de liens avec des cybercriminels.

Une autre tendance observée est le partage d'outils entre différents modes opératoires réputés liés à des États. C'est notamment le cas de ShadowPad [2] qui est utilisé par plusieurs modes opératoires d'attaquants (MOA) , plus particulièrement APT41 et Tonto Team [11] . Cette utilisation partagée d'un même outil, qui suggère une coopération entre différents MOA ou l'existence d'un fournisseur commun, complique nécessairement la caractérisation des activités et leur imputation à un MOA particulier. Cette utilisation partagée a également été observée avec PlugX [12] .

Comme de nombreux cybercriminels, des attaquants de niveau étatique ont recours à la technique du *living-off-the-land* (LOTF) qui consiste à utiliser des outils déjà présents sur le réseau de la victime, notamment des outils d'administration comme PowerShell, pour arriver à leurs fins. Ainsi, ils sont plus difficiles à détecter car ils n'utilisent peu ou pas d'outils caractéristiques d'activités malveillantes. Outre une rationalisation des coûts, ce recours à des outils non-signants, partagés ou exploités depuis le réseau de la victime, permet également de nier de façon plausible toute implication en ne permettant pas une caractérisation précise des activités. C'est particulièrement le cas lors de l'emploi de rançongiciels par des modes opératoires étatiques à des fins lucratives et non de sabotage. À ce titre, plusieurs groupes d'attaquants supposément liés aux intérêts nord-coréens emploieraient des rançongiciels à des fins lucratives tandis que d'autres utiliseraient ce type de code afin d'effacer leurs traces ou dissimuler leur véritable objectif.

En corollaire de cet emprunt de techniques cybercriminelles par des acteurs étatiques, les cybercriminels montent également en compétence atteignant un niveau de sophistication parfois comparable à celui d'attaquants de niveau étatique. Les gains financiers accumulés lors de précédentes opérations leur permettraient des opérations plus ambitieuses et plus longues. Certains groupes cybercriminels sont également en mesure de découvrir et d'exploiter des vulnérabilités inconnues ou *0-Day*, qui étaient historiquement l'apanage de groupes dits étatiques ou d'entreprises spécialisées [13].

Cette porosité entre différents profils d'attaquants peut également profiter à d'autres catégories d'attaquants, notamment les hacktivistes. Un premier cas d'utilisation d'un rançongiciel à des fins hacktivistes a été identifié en Inde en 2021 : le rançongiciel Sarbloh a été utilisé dans le contexte d'une protestation contre une réforme agraire du gouvernement [14].

2. Plateforme d'attaque modulaire permettant d'ouvrir et maintenir un accès distant à un système compromis.

1.3. Des capacités privées qui se développent rapidement

La récente actualité liée aux révélations sur les cibles des clients du système Pegasus commercialisé par la société israélienne NSO Group a permis une réelle prise de conscience de la menace que peuvent représenter certaines entreprises privées. Pourtant le marché existe depuis plus d'une décennie et les entreprises qui y prennent part sont aussi bien implantées que discrètes sur leurs activités et leur clientèle.

Plusieurs offres de services sont possibles : des outils clé en main, de l'expertise humaine ou encore des capacités telles que des méthodes d'exploitation de vulnérabilités *0-Day*. Si ces services sont généralement réservés à des clients étatiques dans le cadre de la lutte contre le terrorisme et la criminalité organisée, les dernières révélations suggèrent un dévoiement de l'utilisation de ces outils à des fins d'espionnage stratégique et politique à l'encontre d'autres cibles telles que des journalistes, des défenseurs des droits de l'homme et de hauts responsables [15] ainsi que d'entreprises détenant des données à caractère personnel comme des opérateurs de communications électroniques ou des entreprises du secteur des transports. Ces services varient de l'utilisation d'applications vérolées en passant par celle d'outils d'attaques plus sophistiqués comme CobaltStrike, jusqu'à l'exploitation de vulnérabilités *0-Day* sans interaction nécessaire de la cible (*0-Click*). Enfin, le recours à une tierce partie, *a fortiori* privée, peut générer un certain sentiment d'impunité qui peut expliquer le ciblage décomplexé de certains commanditaires.

Le développement et la multiplication de ce type d'entreprises augmentent également le risque qu'elles fassent elles-mêmes l'objet d'attaques informatiques amenant à la divulgation d'outils d'attaques potentiellement sophistiqués et à leur prolifération. Pour mémoire, ce fut notamment le cas de la société italienne Hacking Team victime d'une exfiltration de données et d'outils en 2015. Ces outils ont été exploités jusqu'en 2020 par des acteurs réputés liés à des États et des cybercriminels.

Enfin, ces services parfois très sophistiqués peuvent fournir à de nouveaux commanditaires (étatiques ou non) les moyens de mener des attaques informatiques sans avoir à développer leurs propres capacités et compétences.

2. Des intentions d'espionnage et de sabotage peu visibles, mais toujours préoccupantes

Si les attaques à finalité lucrative ont occupé le devant de la scène au cours des derniers mois, il est important de rappeler que l'espionnage reste la première finalité poursuivie avec les tentatives de déstabilisation et les actions de sabotage informatiques.

2.1. L'espionnage reste la première finalité poursuivie, notamment en France

La menace d'espionnage stratégique demeure une constante à prendre en compte ; elle touche autant les acteurs institutionnels que privés. La France est particulièrement ciblée par cette menace comme en témoignent les campagnes d'attaques mettant en œuvre les modes opératoires Sandworm [16], Nobelium [17] ou encore APT31 [10] en 2020-2021. **En 2021, sur les 17 opérations de cyberdéfense traitées par l'ANSSI, 14 étaient liées à des opérations d'espionnage informatique, impliquant pour 9 d'entre elles des modes opératoires réputés chinois. De même, sur 8 incidents majeurs, 5 concernent des MOA réputés chinois.**

Le détournement de cadres juridiques étrangers liés à la cybersécurité peut également faciliter ces actions d'espionnage visant à capter des données à caractère personnel des citoyens français et/ou des données appartenant à des entreprises françaises implantées à l'étranger. Si les dispositifs législatifs relatifs à la cybersécurité se multiplient dans le monde, plusieurs cas de détournement à des fins d'espionnage de dispositifs légaux sans lien avec la cybersécurité ont été rapportés ou soupçonnés. Ainsi certaines versions du logiciel GoldenTax, imposé en Chine, ont embarqué une porte dérobée permettant un accès furtif aux systèmes d'information de plusieurs entreprises [18]. De plus, l'extraterritorialité de certaines législations étrangères en matière de sécurité nationale [3], une notion

3. ITAR, FISA ou le Cloud Act par exemple, ou encore loi sur le renseignement en république Populaire de Chine.

susceptible d'interprétation large, fait peser un risque supplémentaire sur la confidentialité des données et sur la disponibilité des infrastructures numériques.

Cette menace de détournement est susceptible de se multiplier à mesure que les États s'emparent des problématiques cyber au travers de moyens législatifs et règlementaires.

2.2. Le ciblage d'infrastructures critiques à des fins de sabotage demeure une menace constante

Des secteurs extrêmement critiques comme celui de l'eau en Israël et du transport aux États-Unis ont également fait l'objet d'attaques informatiques menées dans des objectifs de prépositionnement et sabotage. En avril 2020, plusieurs installations critiques de gestion de l'eau et des eaux usées en Israël ont ainsi été la cible d'attaques coordonnées mais aux conséquences limitées, ultérieurement attribuées à l'Iran [19]. En février 2021, un avis de sécurité conjoint du CISA, FBI, ISAC et EPA [20] indiquait que des attaquants avaient réussi à accéder au système industriel d'une usine de traitement de l'eau potable en Floride. Ils auraient manipulé le niveau d'hydroxyde de sodium dans une potentielle tentative d'empoisonnement. Les attaquants ont notamment tiré parti de la faiblesse des mots de passe utilisés - les mêmes sur plusieurs interfaces et systèmes - et auraient exploité des vulnérabilités de Windows 7.

Le secteur du transport aérien a également fait l'objet d'attaques informatiques à des fins de prépositionnement. En août 2020, une alerte conjointe du CISA et du FBI indiquait que des actions de reconnaissance étaient menées par des acteurs soutenus par des États dans le secteur aérien. Ces actions menées dans un objectif de prépositionnement comprenaient notamment des recherches de vulnérabilité ainsi que des tentatives de récupération d'identifiants et mots de passe.

L'attaque par sabotage informatique contre le port iranien de Shahid Rajaee de mai 2020, quant à elle, a été attribuée aux autorités israéliennes en représailles de l'attaque contre le système d'eau israélien en avril 2020 [19]. Cette attaque aurait stoppé les systèmes de régulation des flux de cargos et marchandises, entrainant la congestion du trafic à l'entrée du port pendant plusieurs jours.

Le ciblage d'infrastructures critiques par des acteurs de niveau étatique devrait continuer, plus particulièrement dans le cadre de tensions géopolitiques exacerbées. Ces acteurs sont également susceptibles d'instrumentaliser des groupes cybercriminels afin de maintenir une possibilité de déni plausible.

2.3. Des attaques informatiques mises à profit d'opérations d'influence et de déstabilisation

Les opérations d'influence et de déstabilisation ne se limitent plus à la simple création de contenus et à la recherche voire la compromission de relais pour en amplifier la diffusion. De plus en plus d'opérations informationnelles s'appuient sur des compromissions informatiques permettant d'exfiltrer des documents authentiques et d'obtenir des accès initiaux à des systèmes d'informations. Ces documents et accès sont ultérieurement utilisés dans le cadre d'opérations, à l'image de la campagne Ghostwriter attribuée à la Russie par l'Allemagne [21] et l'Union européenne [22] et à la Biélorussie par l'éditeur de sécurité FireEye [23]. Les documents exfiltrés peuvent être divulgués en l'état ou modifiés avant diffusion. **Le phénomène n'est pas nouveau mais appelle à une vigilance particulière à l'approche d'échéances électorales majeures en France en 2022.**

3. De nombreuses faiblesses exploitées

3.1. Exploitation massive de vulnérabilités par différents profils d'acteurs malveillants

Encore trop d'organisations n'appliquent pas à temps les correctifs publiés par les éditeurs de logiciel et offrent aux attaquants un vecteur d'infection initiale relativement aisé à mettre en œuvre sur les systèmes exposés sur Internet. Dès la mise à disposition d'une méthode d'exploitation, en l'espace de quelques jours voire de quelques heures, l'exploitation de vulnérabilités peut être industrialisée notamment grâce à l'identification d'instances vulnérables par le biais de scans massifs et servir des finalités diverses, depuis l'espionnage informatique jusqu'à des attaques à finalité lucrative. C'est notamment le cas des vulnérabilités Exchange dont l'exploitation par de nombreux modes opératoires a fait l'objet de nombreuses publications. L'exploitation de vulnérabilités sur des équipements réseaux (notamment PulseSecure et Citrix) sont communes et permettent régulièrement des attaques par rançongiciel.

Quelques vulnérabilités majeures (Exchange, Log4j, PulseSecure) ont particulièrement marqué l'année 2020-2021. Elles ont pleinement mobilisé l'ANSSI et ses bénéficiaires pour s'assurer de leur correction. Il est à noter que ces vulnérabilités majeures ont touché le monde entier. Elles se retrouvent ainsi dans le classement de l'agence homologue de l'ANSSI aux États-Unis, la CISA. Ces vulnérabilités continueront probablement d'être exploitées dans les mois à venir.

CVE les plus exploitées en 2020					
Incidents ANSSI			Incidents CISA		
1	**CVE-2019-19781**	**Citrix**	**1**	**CVE-2019-19781**	**Citrix**
2	**CVE-2019-11510**	**Pulse**	**2**	**CVE-2019-11510**	**Pulse**
3	**CVE-2018-13379**	**Fortinet**	**3**	**CVE-2018-13379**	**Fortinet**
4	CVE-2020-1472	Netlogon	4	CVE-2020-5902	F5-Big IP
5	CVE-2020-5902	F5-Big-Ip	5	CVE-2020-15505	MobileIron
6	CVE-2020-18935	Telerik	6	CVE-2017-11882	Microsoft
7	CVE-2020-15505	MobileIron	7	CVE-2019-11580	Atlassian
8	CVE-2018-7600	Drupal	8	CVE-2018-7600	Drupal
9	CVE-2017-11882	Microsoft	9	CVE-2019-18935	Telerik
			10	CVE-2019-0604	Microsoft
			11	CVE-2020-0787	Microsoft
			12	CVE-2020-1472	Netlogon

Fig. 3.1. – Vulnérabilités les plus exploitées en 2020 dans le cadre des incidents traités par l'ANSSI et la CISA[4].

4. Pour mémoire, la CISA (Cybersecurity and Infrastructure Security Agency) est l'agence fédérale américaine en charge de la coordination des actions de cyberdéfense des États-Unis.

CVE les plus exploitées en 2021					
Incidents ANSSI			Incidents CISA		
1	**CVE-2021-26855**	**Microsoft Exchange**	**1**	**CVE-2021-26855**	**Microsoft Exchange**
2	**CVE-2021-26857**		**2**	**CVE-2021-26857**	
3	**CVE-2021-26858**		**3**	**CVE-2021-26858**	
4	**CVE-2021-27065**		**4**	**CVE-2021-27065**	
5	CVE-2018-13379	Fortinet	5	CVE-2021-22893	Pulse
6	CVE-2021-21985	VMWare	6	CVE-2021-22894	
7	CVE-2021-22893	Pulse	7	CVE-2021-22899	
			8	CVE-2021-22900	
			9	CVE-2021-27101	Accellion
			10	CVE-2021-27102	
			11	CVE-2021-27103	
			12	CVE-2021-27104	
			13	CVE-2021-21985	VMWare
			14	CVE-2018-13379	Fortinet
			15	CVE-2020-12812	
			16	CVE-2019-5591	

Fig. 3.2. – Vulnérabilités les plus exploitées en 2021 dans le cadre des incidents traités par l'ANSSI et la CISA.

L'année 2020-2021 a également vu l'explosion du nombre de vulnérabilités *0-Day* activement exploitées. Selon l'équipe d'analyse de la menace de Google *Threat Analysis Group* (TAG) en juillet 2021, 33 vulnérabilités de ce type avaient été exploitées avant la mise à disposition d'un correctif, contre 25 en 2020 et 20 en 2019. Plusieurs phénomènes expliquent cette explosion : l'amélioration de la détection et des efforts de partage d'information, mais aussi l'augmentation des capacités techniques des attaquants potentiellement soutenue par le développement de l'écosystème des entreprises commercialisant ce type de vulnérabilités. Le détournement de la législation chinoise sur les vulnérabilités, qui contraint les entreprises à signaler les vulnérabilités aux autorités chinoises, laisse craindre une identification facilitée de vulnérabilités *0-Day* par des groupes d'attaquants chinois.

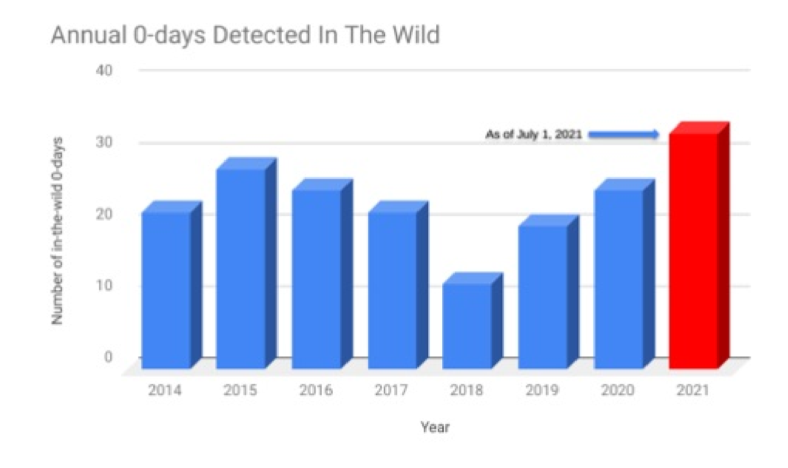


Fig. 3.3. – Évolution du nombre de vulnérabilités *0-Day* exploitées entre 2014 et juillet 2021 selon Google TAG [24]

Si aucun produit logiciel ou matériel n'est imperméable aux vulnérabilités, des mesures existent pour compliquer et éviter leur exploitation à grande échelle. Outre des échanges plus nombreux au sein des communautés dédiées notamment lors de la divulgation d'une méthode d'exploitation, une application prioritaire des correctifs sur les systèmes exposés sur Internet, ou à défaut la mise en œuvre de mesures de contournement, doit être envisagée.

De manière générale, minimiser les possibilités de rebond depuis un serveur hébergeant un applicatif vers un réseau interne passe par un filtrage sortant strict et par le maintien à jour de l'inventaire des comptes de service utilisés. Ces comptes doivent également minimiser leurs privilèges valables à l'échelle du réseau interne. Dans le cas d'un Active Directory, cela signifie que ces comptes ne doivent pas avoir de privilèges de type « Administrateur du domaine », mais être limités :

- idéalement à des privilèges d'utilisateurs standard ;
- de manière exceptionnelle à des privilèges d'administration locaux valables uniquement sur les serveurs hébergeant le produit.

L'ANSSI vous invite à consulter les guides « Cartographie du système d'information » (`https://www.ssi.gouv.fr/administration/guide/cartographie-du-systeme-dinformation/`), « Guide d'hygiène informatique » (`https://www.ssi.gouv.fr/administration/guide/guide-dhygiene-informatique/`) ainsi que l'analyse des « 10 vulnérabilités les plus observées par l'agence en 2021 » (`https://www.cert.ssi.gouv.fr/actualite/CERTFR-2022-ACT-008/`).

3.2. L'exploitation à des fins malveillantes des nouveaux usages numériques comme le Cloud

Amorcé depuis plusieurs années, le recours aux services de *Cloud* s'est particulièrement accéléré au cours des deux dernières années dans les secteurs public et privé, la crise sanitaire ayant agi comme un catalyseur. Cette généralisation augmente mécaniquement le niveau de menace pesant sur ses utilisateurs. En effet, des défauts de sécurisation des données ou de conteneurs sont encore trop souvent rapportés. Entre octobre 2020 et février 2021, Palo Alto a ainsi détecté plus de 2100 instances *cloud* non sécurisées et aisément accessibles [25].

La puissance de calcul qu'offrent les instances *cloud* représente également une cible d'intérêt pour des attaquants qui chercheraient à la détourner à leur profit, notamment pour du minage de cryptomonnaies. Le groupe cybercriminel « TeamTNT » s'est ainsi spécialisé dans le ciblage d'environnements *cloud* à des fins de cryptominage [26], tout comme le groupe « Rocke », réputé chinois, s'est spécialisé dans le cryptominage clandestin sur des serveurs *cloud*. Il exploite ainsi des vulnérabilités sur ces serveurs, qui permettent d'installer une porte dérobée à partir de laquelle les attaquants déploient des cryptomineurs, mettent fin à d'éventuels autres processus de cryptominage antérieurs et empêchent l'installation de nouveaux codes malveillants [27].

Le *Cloud* offre par ailleurs des moyens de propagation sans code malveillant au sein du système d'information ciblé. En effet, de nombreux services de partage de documents et de travail collaboratif permettent une reconnexion facile des utilisateurs sur leurs services, après une authentification initiale. Le même jeton d'authentification peut être utilisé pour tous les matériels d'un utilisateur. Une menace grandissante concerne l'accès à ces jetons d'authentification, les attaquants tentant de récupérer ces derniers par ingénierie sociale. Une fois intercepté et copié par un attaquant, le jeton peut être utilisé depuis un autre appareil sans être détecté. Une autre technique de vol de jeton consiste à installer sur le système de fichier de la cible un jeton connecté à un compte contrôlé par l'attaquant. Lorsque la victime procède à la synchronisation automatique de son dossier dans le *Cloud*, elle le fait alors avec le dossier de l'attaquant et non le sien. L'attaquant peut ainsi récupérer le jeton authentique et le réutiliser à distance et discrètement, tout en effaçant les traces de sa compromission [28].

L'ANSSI vous invite à consulter les guides « Recommandations relatives à l'authentification multifacteur et aux mots de passe » (https://www.ssi.gouv.fr/administration/guide/recommandations-relatives-a-lauthentification-multifacteur-et-aux-mots-de-passe/) et « Recommandations pour la sécurisation de la mise en œuvre du protocole OpenID Connect » (https://www.ssi.gouv.fr/administration/guide/recommandations-pour-la-securisation-de-la-mise-en-oeuvre-du-protocole-openid-connect/).

Le Cloud peut être également source de contraintes et difficultés dont les utilisateurs ne sont pas forcément conscients. Le manque de maitrise de l'infrastructure et la forte dépendance au fournisseur de services, ainsi que des modalités de partage de responsabilité parfois opaques peuvent constituer un obstacle supplémentaire dans l'éventualité d'une compromission. Les difficultés d'intervention et d'investigation, de détection et de remédiation doivent donc être prises en compte.

Bien évidemment, les principes et les bonnes pratiques de sécurité s'appliquent également aux technologies Cloud, notamment en ce qui concerne les mesures de cloisonnement, d'authentification, de journalisation, d'administration ou encore d'externalisation. Il est également rappelé la pertinence d'une démarche de maîtrise des risques (comme EBIOS RISK MANAGER) dans ce contexte.

Enfin, les aspects juridiques et contractuels peuvent être une source de menace supplémentaire. La localisation des données et l'extraterritorialité de certaines législations peuvent avoir des conséquences en matière de protection des données et de souveraineté. La prépondérance d'acteurs étrangers supplémentaires sur le marché européen pourrait augmenter la menace juridique associée au Cloud. Face à ces risques, l'ANSSI a créé dès 2016 la qualification de sécurité « SecNumCloud » à destination des prestataires de *Cloud*. En octobre 2021, une version mise à jour de ce référentiel d'exigences a été publiée sur le site de l'ANSSI pour appel à commentaires. Le futur schéma de qualification SecNumCloud prévoit notamment des exigences organisationnelles et techniques visant à se prémunir des lois à portée extraterritoriale qui permettraient à un pays non européen d'accéder à tout ou partie des données et des traitements hébergés par un offreur.

3.3. Des attaques indirectes via la supply chain de plus en plus courantes

Cette technique est éprouvée et exploitée par plusieurs acteurs étatiques et des cybercriminels depuis au moins 2016. Toutefois, l'ensemble de la communauté cyber observe une tendance largement à la hausse du recours à cette technique d'attaque indirecte. Selon l'ENISA, entre janvier 2020 et juillet 2021, 24 attaques sur la *supply chain* ont été rapportées et documentées [29]. Cette méthode présente un risque de propagation rapide d'une attaque qui peut parfois concerner un secteur d'activité entier ou une zone géographique précise notamment lorsque l'attaque cible une entreprise de service numérique (ESN) locale ou spécialisée dans un secteur d'activité particulier.

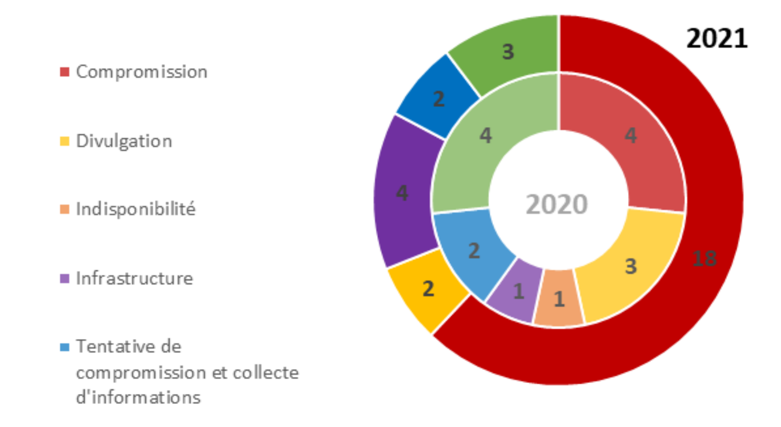


Fig. 3.4. – Comparatif des types d'incidents traités par l'ANSSI et affectant les ESN en 2020 et 2021.

Cette opportunité continuera à se présenter notamment avec la numérisation croissante de la *supply chain*. Au niveau européen, la France plaide donc en faveur d'une imposition d'exigences de sécurité aux acteurs incontournables du numérique que sont les ESN dans le cadre de la révision de la directive NIS (*Network and information Security*) afin de limiter l'effet domino que pourrait entrainer leur compromission.

3.4. Faible sécurisation des données entrainant des leaks massifs

Ces divulgations peuvent être classées en quatre grandes catégories : les divulgations de données dans le cadre d'attaques par rançongiciel ; les divulgations motivées idéologiquement (hacktivisme) [30] ou dans le cadre d'opérations de déstabilisation [31] ; les divulgations de données à des fins de revente ; et enfin les divulgations par négligence.

Ces divulgations peuvent en outre être réutilisées pour mener des attaques via la *supply chain* et pour mener des campagnes de hameçonnage. Elles peuvent conduire à une atteinte au secret des affaires voire à la sécurité nationale, lorsque des données d'entreprises (contrats, clients, *etc.*) ou classifiées sont publiées. Les conséquences en matière de réputation sont souvent majeures.

La valeur accordée aux données par les États, les entreprises privées, les acteurs cybercriminels ou toute autre catégorie d'acteur conduira les attaquants à poursuivre ces divulgations. Une veille régulière à l'image de celles opérées dans le cadre d'une démarche d'intelligence économique peut permettre d'identifier au plus tôt ces divulgations. Des services gratuits en ligne (HaveIbeenPwned par exemple) permettent également de vérifier si une adresse courriel, un identifiant ou un mot de passe ont déjà fait l'objet d'une divulgation. Ces outils sont toutefois utilisés de manière réactive ou *post mortem* et doivent être complétés et précédés par une sensibilisation aux mots de passe forts, à l'usage systématique de gestionnaires de mot de passe et l'activation généralisée de procédés d'authentification à multiples facteurs.

4. Conclusion

Dans les prochains mois, de nouvelles opportunités se présenteront aux attaquants notamment en France. Les intentions associées seront hétérogènes, allant de la déstabilisation à l'influence en passant par l'espionnage et le gain financier. Si l'exploitation de vulnérabilités *0-day* reste imprévisible, les élections législatives et présidentielles de 2022 ainsi que la tenue de la coupe du monde rugby en 2023 et des Jeux olympiques en France en 2024 seront autant d'évènements que les attaquants chercheront à exploiter. Les cibles potentielles sont multiples et présentent des niveaux de maturité en sécurité des systèmes d'information très variables - médias, partis politiques, organisations gouvernementales et publiques, think tanks, entreprises du numérique, opérateurs critiques, etc. - et **appellent à une vigilance particulière de l'ensemble des parties prenantes**.



A. Bibliographie

[1] CERT-FR. *Le Code Malveillant Dridex : Origines et Usages*. 25 mai 2020.
URL : https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-005.pdf.

[2] Security Affairs. *Evil Corp Rebrands Their Ransomware, This Time Is the Macaw LockerSecurity Affairs*. 21 octobre 2021.
URL : https://securityaffairs.co/wordpress/123661/cyber-crime/evil-corp-macaw-locker.html.

[3] CERT-FR. *Le Malware-as-a-Service Emotet*. 2 novembre 2020.
URL : https://www.cert.ssi.gouv.fr/cti/CERTFR-2020-CTI-010/.

[4] Krebs On Security. *Meet the World's Biggest 'Bulletproof' Hoster*. 16 juillet 2019.
URL : https://krebsonsecurity.com/2019/07/meet-the-worlds-biggest-bulletproof-hoster/.

[5] Krebs On Security. *Amid an Embarrassment of Riches, Ransom Gangs Increasingly Outsource Their Work*. 9 octobre 2020.
URL : https://krebsonsecurity.com/2020/10/amid-an-embarrassment-of-riches-ransom-gangs-increasingly-outsource-their-work/.

[6] Intel 471. *Bulletproof Hosting : How Cybercrime Stays Resilient*. 23 février 2021.
URL : https://intel471.com/blog/bulletproof-hosting-yalishanda-ransomware-banking-trojans-information-stealers.

[7] Department of Justice. *Three Members of Notorious International Cybercrime Group Fin7*. 1er août 2018.
URL : https://www.justice.gov/opa/pr/three-members-notorious-international-cybercrime-group-fin7-custody-role-attacking-over-100.

[8] Bleeping Computer. *US Declares State of Emergency after Ransomware Hits Largest Pipeline*. 10 mai 2021.
URL : https://www.bleepingcomputer.com/news/security/us-declares-state-of-emergency-after-ransomware-hits-largest-pipeline/.

[9] Computerworld. *US to Give Ransomware Attacks Similar Priority as Terrorism, Official Says*. 4 juin 2021.
URL : https://www.itnews.com.au/news/us-to-give-ransomware-attacks-similar-priority-as-terrorism-official-says-565470.

[10] CERT-FR. *Campagne d'attaque Du Mode Opératoire APT31 : Description, Contre-Mesures et Code*. 15 décembre 2021.
URL : https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-012/.

[11] MITRE ATT&CK. *ShadowPad Software*. 26 avril 2021.
URL : https://attack.mitre.org/software/S0596/.

[12] MITRE ATT&CK. *PlugX Software*. 20 juin 2020.
URL : https://attack.mitre.org/software/S0013/.

[13] The Hacker News. *REvil Used 0-Day in Kaseya Ransomware Attack, Demands $70 Million Ransom*. 6 juillet 2021.
URL : https://thehackernews.com/2021/07/revil-used-0-day-in-kaseya-ransomware.html.

[14] Bleeping Computer. *New Sarbloh Ransomware Supports Indian Farmers' Protest*. 8 mars 2021.
URL : https://www.bleepingcomputer.com/news/security/new-sarbloh-ransomware-supports-indian-farmers-protest/.

[15] Le Monde. *Comment les services de renseignement français ont traqué Pegasus après les révélations du « Monde »*. 19 novembre 2021.
URL : https://www.lemonde.fr/pixels/article/2021/11/19/comment-le-renseignement-francais-a-traque-pegasus-apres-les-revelations-du-monde_6102638_4408996.html.

[16] CERT-FR. *Campagne d'attaque Du Mode Opératoire Sandworm Ciblant Des Serveurs Centreon*. 15 février 2021.
URL : https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-004/.

[17] CERT-FR. *Campagnes d'hameçonnage Du Mode Opératoire d'attaquants Nobelium*. 6 décembre 2021.
URL : https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-010/.

[18] Trustwave. *The Golden Tax Department and the Emergence of GoldenSpy Malware*. 25 juin 2020.
URL : https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/the-golden-tax-department-and-the-emergence-of-goldenspy-malware/.

[19] The Washington Post. « Cyberattack on Iranian Port Is Attributed to Israel ». 18 mai 2020.
URL : https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html.

[20] CISA. *Compromise of U.S. Water Treatment Facility*. 11 février 2021.
URL : https://www.cisa.gov/uscert/ncas/alerts/aa21-042a.

[21] Infosecurity Magazine. *Germany Accuses Russia of Election Meddling Through Cyber-Attacks*. 7 septembre 2021.
URL : https://www.infosecurity-magazine.com/news/germany-russia-election-meddling/.

[22] Conseil européen. *Declaration by the High Representative on Behalf of the European Union on Respect for the EU's Democratic Processes*. 24 septembre 2021.
URL : https://www.consilium.europa.eu/en/press/press-releases/2021/09/24/declaration-by-the-high-representative-on-behalf-of-the-european-union-on-respect-for-the-eu-s-democratic-processes/.

[23] FireEye. *Ghostwriter Update : Cyber Espionage Group UNC1151 Likely Conducts Ghostwriter Influence Activity*. 28 avril 2021.
URL : https://www.fireeye.com/content/dam/fireeye-www/blog/pdfs/unc1151-ghostwriter-update-report.pdf.

[24] Google TAG. *How We Protect Users from 0-Day Attacks*. 14 juillet 2021.
URL : https://blog.google/threat-analysis-group/how-we-protect-users-0-day-attacks/.

[25] Palo Alto - Unit42. *Unsecured Kubernetes Instances Could Be Vulnerable to Exploitation*. 23 avril 2021.
URL : https://unit42.palonetworks.com/unsecured-kubernetes-instances/.

[26] Intezer. *Intezer - Attackers Abusing Legitimate Cloud Monitoring Tools to Conduct Cyber Attacks*. 8 septembre 2020.
URL : https://www.intezer.com/blog/cloud-workload-protection/attackers-abusing-legitimate-cloud-monitoring-tools-to-conduct-cyber-attacks/.

[27] Palo Alto Networks. *Malware Used by "Rocke" Group Evolves to Evade Detection by Cloud Security Products*. 17 janvier 2019.
URL : https://unit42.paloaltonetworks.com/malware-used-by-rocke-group-evolves-to-evade-detection-by-cloud-security-products/.

[28] Help Net Security. *Beware the Man in the Cloud : How to Protect against a New Breed of Cyberattack*. 21 janvier 2019.
URL : https://www.helpnetsecurity.com/2019/01/21/mitc-attack/.

[29] ENISA. *Threat Landscape for Supply Chain Attacks*. 29 juillet 2021.
URL : https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks.

[30] actu.fr. *Cyberattaque de l'AP-HP à Paris : un étudiant mis en examen, les données publiées sur internet*. 11 octobre 2021.
URL : https://actu.fr/ile-de-france/paris_75056/cyberattaque-de-l-ap-hp-a-paris-un-etudiant-mis-en-examen-les-donnees-publiees-sur-internet_45576995.html.

[31] Ars Technica. *NSA Employee Who Brought Hacking Tools Home Sentenced to 66 Months in Prison*. 25 septembre 2018.
URL : https://arstechnica.com/tech-policy/2018/09/nsa-employee-who-brought-hacking-tools-home-sentenced-to-66-months-in-prison/.

1.9.1 - 9 mars 2022

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51 boulevard de la Tour-Maubourg, 75700 PARIS 07 SP
www.cert.ssi.gouv.fr / cert-fr.cossi@ssi.gouv.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
SGDSN